

**WRITTEN TESTIMONY OF  
JEFFREY J. TRIBIANO  
DEPUTY COMMISSIONER FOR OPERATIONS SUPPORT  
AND  
SILVANA GINA GARZA  
CHIEF INFORMATION OFFICER  
INTERNAL REVENUE SERVICE  
BEFORE THE  
HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE  
SUBCOMMITTEE ON HEALTHCARE, BENEFITS AND ADMINISTRATIVE  
RULES AND  
SUBCOMMITTEE ON GOVERNMENT OPERATIONS  
ON IRS MANAGEMENT CHALLENGES  
OCTOBER 25, 2017**

**I. INTRODUCTION**

Chairmen Jordan and Meadows, Ranking Members Krishnamoorthi and Connolly and members of the Subcommittees, thank you for the opportunity to appear before you today to testify on recent IRS management challenges.

Before discussing the three specific areas we have been asked to address, we wanted to provide the Subcommittees with an overview of the IRS's current approach to managing risks within our operations.

The IRS has been working for several years to ensure risks are managed more effectively throughout the organization. In 2014, we established an agency-wide enterprise risk management program, creating risk management liaisons in each area of our operations, and providing for the regular identification and analysis of risks to be eliminated or managed across the agency.

We are aware that actions the IRS takes have the potential to affect millions of taxpayers. So, for the IRS, a risk management program provides a framework for regularly reviewing existing risks and identifying new ones, so that problems can be dealt with in a timely manner. The goal of our program is to stay ahead of the curve and anticipate risks whenever possible, to identify and fix problems when they arise quickly, and to be transparent about the entire process.

We are working to create a culture where employees are encouraged to think of themselves as risk managers and to report any issues or problems that occur. We are encouraging the further flow of information from front-line employees up through the organization as well as out to the front line from senior managers. As part of this program, each of the IRS business divisions established a Risk Management Process to enable certain issues to be elevated to the executive

leadership for review and discussion. This new and expansive process reduces the risk of overlooking sensitive issues.

## **II. MODERNIZING IRS INFORMATION TECHNOLOGY SYSTEMS**

One issue we have been asked to address is the need to modernize our information technology (IT) systems.

The IRS's Information Technology Division provides critical support to the agency's dual mission of providing taxpayer service and enforcing the tax laws. In allocating resources for these efforts, our highest priorities are delivering the filing season, implementing congressional mandates and ensuring that our computer systems and the taxpayer data they hold remain protected.

At the same time, we continue to invest in modernizing our tax administration applications in several areas, including the Return Review Program, the Customer Account Data Engine (CADE2) and Enterprise Case Management (ECM) – which are discussed in more detail later in this testimony – and Web Apps. This also includes investments in modernizing critical infrastructure such as our Portal Operations and Enterprise Storage Service, both of which take advantage of managed services.

To continue delivering on our priorities and modernization efforts, it is critical that the agency's IT infrastructure components be up-to-date. But while we have consistently delivered successful filing seasons and implemented legislative mandates, the risk posed by our aged infrastructure is threatening this success. Approximately 64 percent of IRS hardware is aged, and 32 percent of supporting software is two or more releases behind the industry standard, with 15 percent more than four releases behind.

While we have taken steps to maintain our most critical systems, the IRS needs to upgrade its IT infrastructure, not only to help ensure reliable and modern taxpayer services, but also to mitigate risks to the system. We are concerned that the potential for a catastrophic system failure is increasing as our infrastructure continues to age. Thus, replacing this aging IT infrastructure is a high priority for the IRS.

The IRS remains very appreciative of Treasury Secretary Mnuchin's support for the IRS to have the appropriate resources available to upgrade our IT systems. In fact, a priority in the President's Fiscal Year (FY) 2018 Budget is helping the IRS improve information services by addressing its aged infrastructure.

The President's budget request includes \$3.9 billion for operations support. Within that total, \$2.07 billion is allocated for information services, which is \$216.1 million, or 11.6 percent, above the FY 2017 enacted level. This funding

will allow the IRS to take the initial steps needed to bring our IT infrastructure up to date.

## **Taxpayer Services Supported by IT Systems**

### ***Delivering the Tax Filing Season***

The most visible taxpayer service the IRS provides is the delivery of a smooth, problem-free tax filing season, so that people can file their returns and receive their refunds as quickly and easily as possible. Our IT systems process approximately 150 million individual income tax returns and more than \$300 billion in refunds to individuals each year.

Our ability to effectively manage the IRS's IT systems, despite our aged infrastructure, is evidenced by the fact that the IRS continues to deliver smooth filing seasons, amid steady growth both in the number of returns filed and the percentage of electronically filed returns over the past decade, and a number of complex tax law changes.

Today, nearly 90 percent of individual income tax returns are filed electronically. Return processing has gone smoothly, even in years where passage of tax legislation late in the year has required the IRS to move quickly to update our systems to accommodate tax changes enacted by Congress.

During the filing season and throughout the year, the IRS provides taxpayer services through a variety of delivery channels to help taxpayers file their tax returns accurately and on time. Here too, our IT systems are an essential component of our service efforts. For example, IT supports our call center operation, which is one of the largest in the country, and which answered more than 64 million taxpayer calls in FY 2016, including automated calls and those using a live assistor.

Our IT systems also support our ability to offer online services, which we continue to expand in response to increasing taxpayer demand. We provide a wealth of tax information on our website, IRS.gov, which was visited more than 500 million times during FY 2016, and more than 490 million times in FY 2017. The IRS recently completed a revamp of IRS.gov to make the site more user-friendly and to make it easier for taxpayers to view site content on their mobile devices.

### ***Protecting Taxpayer Data***

Providing outstanding taxpayer service also involves ensuring that the information taxpayers provide to the IRS will be kept secure. The IRS continues to work to protect our main computer systems from cyber incidents, intrusions and attacks, with our primary focus being on preventing criminals from accessing

taxpayer information stored in our databases, as well as identifying fraud. Our core tax processing systems remain secure, and currently withstand more than one million attempts to maliciously access them each day.

We realize the solutions we have in place today may be insufficient in the future, as criminal enterprises continue to invest to find ways to try to penetrate our systems. They are persistent and have demonstrated their ability to adapt. Their tactics are ever-changing, and so our protections must keep changing as well. We therefore must continue to invest in cybersecurity and find ways to collaborate across government. The supplemental funds that Congress provided over the last two years helped us make great progress, but continued investments are needed.

### ***Protecting Taxpayers against Identity Theft and Refund Fraud***

Along with protecting the taxpayer data we have, the IRS is also focused on protecting taxpayers who may have had their personal information stolen from outside the tax system by identity thieves, who use this information to file false returns and claim fraudulent refunds. In recent years, we have made steady progress in protecting against identity thieves, by employing information technology to assist in fraud detection.

An important advance that has helped us in the fight against identity theft has been the implementation of the Return Review Program (RRP). RRP is an integrated and unified system that enhances our ability to detect and potentially prevent tax non-compliance. During the 2016 filing season, RRP replaced the legacy Electronic Fraud Detection System (EFDS) in the tax system pipeline as the government's primary line of defense against the perpetration of tax-related identity theft, along with other tax fraud and noncompliance associated with individual tax returns. Continued investment in RRP will allow the IRS to address more sophisticated instances of identity theft more quickly and expand RRP's use to business returns.

Over the past two years, our progress against stolen identity refund fraud has accelerated, thanks to implementation of RRP and the collaborative efforts of the Security Summit, a unique partnership launched in March 2015 that includes the IRS, industry leaders and state tax commissioners. Our collaborative efforts have put in place many new safeguards beginning in the 2016 filing season that produced real results.

Since 2015 we have had fewer fraudulent returns entering our systems, fewer bad refunds going out the door, and fewer tax-related identity theft victims than in previous years. To illustrate, the number of people who reported to the IRS that they were victims of identity theft declined from 698,700 in Calendar Year (CY) 2015 to 376,500 in 2016 – a drop of nearly half.

The decline has continued during 2017. In the first eight months of this year, about 189,000 taxpayers reported they were victims of identity theft, which is a drop of about 40 percent from the same period last year. Taken together, the number of taxpayers over the last two years who reported being victims of tax-related identity theft has dropped by nearly two-thirds.

### ***Providing for the Future of Taxpayer Service***

In addition to ensuring that the basic taxpayer experience with the IRS is safe, secure and functional, the agency has been working for several years on longer-term improvements to the taxpayer experience and tax administration. In this effort, the IRS relies heavily on our information technology systems to help carry out these improvements.

Our goal is to have a more proactive and interactive relationship with taxpayers and tax professionals by offering them the services, tools and support they want, in ways that are both innovative and secure. We are working to catch up with the kinds of online and virtual interactions people already use in their daily lives to communicate with banks, retailers, medical providers and many others.

A major part of our initiative is developing an online account where taxpayers, or their representatives, can log in securely, get information about their account, and interact with the IRS as needed, including self-correcting some issues.

In December 2016, we took the first step toward this with the launch of an application on IRS.gov that provides information to taxpayers who have straightforward balance inquiries. Since its launch, this new tool has been used by taxpayers more than 1.7 million times. We recently added another feature that lets taxpayers see recent payments posted to their account. These balance-due and recent-payment features, when paired with existing online payment options, have increased the availability of secure, self-service interactions with the IRS through IRS.gov.

These are important steps, and over time, we will be looking to add other features to this platform as they are developed and tested with taxpayers and tax professionals. One of these features which is now in testing is Taxpayer Digital Communications. Taxpayer Digital Communications is intended to provide a secure online messaging capability so that taxpayers, their authorized representatives and IRS employees can correspond electronically and resolve issues more quickly than through traditional mail while maintaining security.

### ***Providing the Taxpayer an Effective Point of Contact***

Along the way, the IRS has come to realize that our efforts to move toward the future need to involve more than just online interactions between the IRS and taxpayers and their representatives. Therefore, our efforts to use technology more efficiently has evolved to cover the entire scope of the taxpayer experience,

whether on-line or in person, and poses considerable opportunities for us and for taxpayers.

Our present case management system treats each issue involving a taxpayer as a separate case. And those cases are handled throughout the agency by more than 60 aging case management systems that often don't communicate with each other. So, when taxpayers with more than one pending issue call the IRS, they must be transferred from one area to another to get the assistance they need.

We are in the process of developing an Enterprise Case Management (ECM) system that will modernize, upgrade and consolidate our existing separate case management systems and give authorized IRS employees the ability to see information relevant to the taxpayer's range of issues, including prior communication with the taxpayer.

Another initiative that will help the IRS improve the taxpayer experience is the Event Driven Architecture (EDA) framework, which will allow us to process tax returns in near-real time. Once in place, the EDA framework will allow the IRS to, for example, notify taxpayers of potential errors on a return as soon as it is filed, and let taxpayers quickly correct certain return errors online – a major advance over the current system, in which the IRS corresponds with taxpayers by mail regarding potential problems in their returns.

These and other improvements depend upon our continued development of the Customer Account Data Engine (CADE 2), which is our centralized database for all individual taxpayer accounts and allows an IRS employee who is helping resolve a taxpayer's issue to easily access the taxpayer's information.

When fully implemented, CADE2 will replace the legacy Individual Master File (IMF), which historically has been the primary data source for individual taxpayer accounts. CADE2 is replacing the IMF in three major steps. It is important to note that this is a complex, multistep process – not a single, easily accomplished action. The steps we have undertaken thus far have already provided important improvements to our ability to interact with taxpayers efficiently and effectively.

### **Challenges to Modernizing IT Systems**

In recent years, Congress has tasked the IRS with implementing several legislative requirements. Satisfying these requirements has involved significant IT investments, diverting staff and resources that otherwise could have been used to continue modernizing our major IT systems and aging IT infrastructure.

These legislative requirements include those stemming from: The Affordable Care Act (ACA); the Foreign Account Tax Compliance Act (FATCA); the Achieving a Better Life Experience (ABLE) Act, which includes a new certification requirement for professional employer organizations; reauthorization of the

Health Coverage Tax Credit (HCTC); a private debt-collection program; and a registration requirement for newly created 501(c)(4) organizations.

Changes in tax law also often require significant IT resources to ensure proper implementation, especially when they are made retroactive. Recently, for example, Congress passed tax relief for victims of the hurricanes that struck the U.S. mainland and Puerto Rico. We are still evaluating the time it will take to implement these changes

The IRS also needs to be able to attract individuals from the private sector with highly specialized IT skills and expertise, particularly for our leadership positions in IT. In the past, the IRS successfully recruited such individuals using streamlined critical pay authority that was first enacted in 1998 and subsequently reauthorized by Congress in 2007 and 2013.

In fact, TIGTA has noted the IRS had appropriately used this authority by adequately justifying the positions, demonstrating the need to recruit or retain exceptionally well-qualified individuals, and adhering to pay limitations. This authority expired at the end of FY 2013 and has not yet been renewed.

The loss of streamlined critical pay authority has created major challenges to our ability to retain employees with the necessary high-caliber expertise in IT and other specialized areas. In fact, there are no longer any executives under streamlined critical pay authority at the IRS. The President's FY 2018 Budget proposes reinstating this authority, and we urge Congress to approve this proposal.

### **III. SHORT-TERM INTERIM CONTRACT WITH EQUIFAX**

Another subject the Subcommittees have asked us to address involves a sole source contract awarded to Equifax in late September after the company announced a major data breach.

The IRS had a contract with Equifax to offer credit monitoring services and another separate contract to provide identity authentication services. During 2017 the IRS re-competed the contract for credit monitoring and the contract was awarded to a new vendor effective October 1, 2017. In addition, the IRS re-competed the contract for identity authentication and the contract was awarded to a new vendor in July 2017.

But Equifax protested our decision on the identity authentication services contract to the Government Accountability Office (GAO). This required us to hold the contract with the new vendor in abeyance until the GAO issued its ruling, which it did on October 16. That ruling upheld our decision to award the contract to a different vendor, and we are now transitioning to that new vendor.

While the GAO decision was still pending, we were faced with the possibility of a lapse in service, because the original contract with Equifax expired on September 30. Thus, on September 29, we entered into a short-term interim contract with Equifax. As the incumbent, Equifax was the only vendor that we could contract with to provide identity authentication services to the IRS until the GAO issued its ruling.

We only took this step after reviewing and determining that there was no indication that the limited data shared under the IRS contract had been compromised. We made this decision to maintain our ability to provide certain online services to taxpayers requiring them to authenticate their identity, particularly online requests for a prior year tax return, "tax transcript." We believed it was important to keep these services available to taxpayers, especially those who were preparing to file tax returns before their extensions ran out on October 16.

Meanwhile, the IRS continued its ongoing review of Equifax's systems and security. On October 12, after receiving new information on Equifax's situation, we took the precautionary step of temporarily suspending this short-term contract.

We took steps to understand and evaluate the impact of the Equifax data breach on IRS systems before we made the decision to enter into the interim contract.

Immediately upon hearing of the Equifax data breach on September 7, the Chief Privacy Officer established an Incident Response Team (comprised of personnel from Wage & Investment, Procurement, IT, Cybersecurity, General Counsel, Risk, Research and Analytics, and Online Service's Identity Assurance) to ascertain the extent of the breach and surrounding issues as well as to keep all stakeholders informed. Furthermore, IT collaborated with the Treasury Inspector General for Tax Administration (TIGTA) Criminal Investigations and IRS Criminal Investigations to form a Security Review Team (SRT). The SRT held several conversations with Equifax and conducted an initial on-site inspection at its headquarters, all of which confirmed no IRS data was compromised and the services provided by Equifax under the contract were not affected.

The suggestion has been made that we had the option to ignore the protest and proceed directly with the new vendor. Such action is available to an agency if there are "urgent and compelling circumstances that significantly affect the interests of the United States," or if performance of the contract is in the best interests of the United States. Since there was no indication that any IRS data was accessed during the Equifax breach, and Equifax had been successfully providing the service in the past, we determined this option was not available.



More generally, the IRS has taken significant steps in recent years to strengthen our tax processing systems to further protect against identity theft and refund fraud. These efforts are part of our Security Summit partnership with state tax administrators and the private-sector tax community.

Our work in this area added new protections for tax returns being filed, including greater authentication measures in our processing systems to verify legitimate tax filers and protect against identity thieves submitting fraudulent tax returns. These additional fraud filters and cross-checks make it harder for identity thieves who have only basic taxpayer information to obtain false refunds. We specifically designed these safety measures to protect against many of the recent large-scale data breaches, such as at Equifax, where criminals obtained such basic information as names and Social Security numbers.

#### **IV. PROCEDURES FOR RE-HIRING FORMER IRS EMPLOYEES**

Another issue the subcommittees have asked us to address involves the procedures we use to rehire former employees.

The IRS is committed to properly evaluating prior performance and conduct issues. We have in place procedures – which we continue to refine – to consider prior performance and conduct in the hiring process to the extent permissible by law, rule and regulation. The IRS hiring process requires our human capital professionals to fully evaluate conduct issues in accordance with [5 CFR 731.202](#) and the Office of Personnel Management’s Suitability Adjudication Handbook. During the selection process, prior performance issues must also be considered before we make final hiring decisions.

To strengthen this process, we have updated our policies and practices, and are continuing to explore additional methods to ensure that we meet hiring needs while considering all prior performance and conduct issues. This includes taking corrective actions in response to the recommendations made in a TIGTA report issued in July. We are on track to complete those actions by the end of October 2017.

Our updated process will allow us to review and document derogatory performance and conduct information on former IRS employees, regardless of the age of that information. Substantiated derogatory information on former employees will be forwarded to the selecting official before a selection is made. The selecting official will document any decision to rehire former employees with prior conduct or performance issues, and our Human Capital Office will maintain the documentation.

Along with these changes, the IRS has also assembled a team to explore additional steps, such as developing a process that will eliminate former IRS

employees with a documented history of misconduct or performance problems from the hiring process.

It is important to note that most of the rehired employees identified in the TIGTA report were seasonal employees who had been hired to support the 2017 filing season. Because our corrective actions will be completed by the end of October 2017, they will be in place before we begin onboarding new employees for the 2018 filing season. After the 2018 filing season, we will review our hiring to gauge the effectiveness of our policy changes.

Chairmen Jordan and Meadows, Ranking Members Krishnamoorthi and Connolly, and Members of the Subcommittees, this concludes our statement, and we would be happy to take your questions.